EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kin-Wah Tong on 11/19/2010.

Claims:

1. (Currently Amended) An internet service provider virtual private network ~~network~~ comprising:

a plurality of edge routers;

a plurality of core routers for allowing communication between the plurality of edge routers;

a virtual private network application in communication with ~~a first one of~~ the plurality of edge routers, the virtual private network application having a first internet protocol address; and

a black-hole router in communication with the plurality of core routers, wherein virtual private network traffic received by the black-hole router is black-holed, the black-hole router for injecting a second ~~IP~~ internet protocol address into the internet service provider virtual private network, the second internet protocol address comprising:

a same internet protocol address as the first internet protocol address;

a higher preference value than the first internet protocol address; and

a community value such that when the second internet protocol address is injected, a selected first number of edge routers of the plurality of edge routers directs ~~direct~~ virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers of the plurality of edge routers directs ~~direct~~ virtual private network traffic addressed for the second internet protocol address to the black-hole router.

2. (Previously Presented) The internet service provider virtual private network of claim 1, wherein the internet service provider virtual private network is a multiprotocol label switching virtual private network.

3. (Previously Presented) The internet service provider virtual private network of claim 1, wherein the black-hole router injects the second internet protocol address in response to a distributed denial of service attack on the virtual private network application.

4. (Currently Amended) The internet service provider virtual private network of claim 1, wherein the community value is changed ~~in real-time~~ by the black-hole router.

5. (Previously Presented) The internet service provider virtual private network of claim 1, wherein the internet service provider virtual private network utilizes a plurality of dynamic routing protocols in combination with a community-based route filtering to propagate the injected second internet protocol address to the plurality of edge routers.

6. (Previously Presented) The internet service provider virtual private network of claim 1 wherein when the selected second number of edge routers directs virtual private network traffic, addressed for the first internet protocol address, to the black-hole router, the black-hole router is for receiving such virtual private network traffic as black-holed-traffic, the black-hole router for analyzing the black-holed traffic in order to determine a ratio of attack traffic to legitimate traffic.

7. (Previously Presented) The internet service provider virtual private network of claim 1, further comprising a route reflector, the route reflector being connected to a different set of edge routers from the plurality of edge routers, the route reflector for updating the plurality of edge routers with route instructions, such route instructions including the injected second internet protocol address.

8. (Currently Amended) An internet service provider network comprising:

a plurality of edge routers;

an application in ~~direct or indirect electrical~~ communication with ~~a first one of~~ the plurality of edge routers;

the application having a first internet protocol address such that virtual private network traffic addressed for the first internet protocol address and entering the internet service provider network at any one of the plurality of edge routers, is routed to the application;

a black-hole router, wherein virtual private network traffic received by the black-hole router is black-holed; and

a router for injecting an instruction into the internet service provider network, such that a select edge router of the plurality of edge routers redirects virtual private network traffic, which is addressed to the first internet protocol address, to the black-hole router, wherein the ~~injected~~ instruction that is injected comprises a routing instruction having a same internet protocol address as the first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value such that when the routing instruction is injected, a selected first number of edge routers of the plurality of edge routers directs virtual private network traffic addressed for the first internet protocol address to the application.

9. (Canceled)

10. (Previously Presented) The internet service provider network of claim 8, wherein the internet service provider network is a multiprotocol label switching virtual private network.

11. (Previously Presented) The internet service provider network of claim 8, wherein the router and the black-hole router are the same device.

12. (Currently Amended) The internet service provider network of claim 8, wherein the ~~injected~~ routing instruction is a border gateway protocol routing instruction.

13. (Previously Presented) The internet service provider network of claim 8, wherein the black-hole router is for receiving redirected traffic from the select edge router and to determine a ratio of attack virtual private network traffic to legitimate virtual private network traffic found in the redirected traffic.

14. (Currently Amended) The internet service provider network of claim 8, wherein the router injects the routing instruction when the application is experiencing a distributed denial of service attack.

15. (Previously Presented) A method of managing a distributed denial of service attack on an application within an internet service provider network, the application having a first internet protocol address, the method comprising:

injecting a border gateway protocol routing instruction into the internet service provider network when the distributed denial of service attack is occurring, the border gateway protocol routing instruction comprising a second internet protocol address having a same internet protocol address as the first internet protocol address, but with a higher preference value than the first internet protocol address and having a community value;

redirecting, at a selected edge router, virtual private network traffic addressed for the second internet protocol address to a black-hole router, wherein the virtual private network traffic received by the black-hole router is black-holed; and

directing, at another edge router, virtual private network traffic addressed for the first internet protocol address to the application that is experiencing the distributed denial of service attack.

16. (Previously Presented) The method of claim 15, wherein the internet service provider network is a multiprotocol label switching virtual private network.

17. (Currently Amended) The method of claim 15, further comprising:

receiving, at the black-hole router, the redirected virtual private network traffic; and

determining an amount of attack traffic ~~therein~~.

18. (Currently Amended) The method of claim 15, further comprising changing, ~~in real-time,~~ a number of selected edge routers that ~~are~~ is redirected.

19. (Previously Presented) The method of claim 15, wherein the injecting the border gateway protocol routing instruction into the internet service provider network is done by providing the border gateway protocol routing instruction to a route-reflector for disseminating the border gateway protocol routing instruction to other route reflectors within the internet service provider network.

Response to Arguments

2. Applicant's arguments, see RCE, filed 10/7/2010, with respect to claims 1, 8, 15 have been fully considered and are persuasive. The Examiner agrees that the claims of this application are directed to VPN application and VPN networks which is different than the patented application. Also, the present claims includes a community value which is used to black-hole the VPN traffic which is different from the patented case. Thus, the statutory double patenting rejection has been withdrawn.

3. The terminal disclaimer filed 10/7/2010 has been accepted and approved. Therefore, the non-statutory double patenting rejection based on App. no. 12/284254 has been withdrawn.

REASONS FOR ALLOWANCE

4. Claims 1-8, and 10-19 have been allowed and been renumbered claims 1-18.

5. The following is an examiner's statement of reasons for allowance: None of the prior art of record teach or suggest the system or method a community value such that when the second internet protocol address is injected, a selected first number of edge routers of the plurality of edge routers directs virtual private network traffic addressed for the first internet protocol address to the virtual private network application and a selected second number of edge routers of the plurality of edge routers directs virtual private network traffic addressed for the second internet protocol address to the black-hole router.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOE CHACKO whose telephone number is (571)270-3318. The examiner can normally be reached on Monday-Friday 8:30am-5pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. C./
Examiner, Art Unit 2456

/Rupal D. Dharia/
Supervisory Patent Examiner, Art Unit 2400